Briefings on HIPAA

HIPAA Security Rule: Facility access controls

by Dom Nicastro

In its August 2024 OCR Cybersecurity Newsletter, HHS talked about the importance of facility access controls. Here's a breakdown of the newsletter followed by a Q&A with a cybersecurity expert.

Importance of facility access controls

HHS noted that only 7% of data security leaders are concerned about breaches from lost or stolen equipment, despite this accounting for 17% of breaches. From 2020 to 2023, OCR reported over 50 large breaches affecting more than 1 million individuals due to stolen devices like workstations, laptops, and medical devices. Loss of critical devices can disrupt healthcare delivery and damage infrastructure, leading to delays and increased recovery costs.

The HIPAA Security Rule aims to ensure the confidentiality, integrity, and availability of ePHI by safeguarding physical access to facilities and electronic information systems. Under the standard addressing facility access controls, organizations are required to implement policies and procedures to limit physical access to electronic information systems while allowing authorized access.

Key implementation specifications

Facility access controls consist of four addressable implementation specifications:

- **Contingency operations:** Maintaining physical security and access to ePHI during emergencies or disasters. Organizations should:
  - Identify who needs access during emergencies
  - Develop processes for expedited or temporary access
  - Establish alternate access methods
  - Plan for monitoring or securing facilities following a disaster
  - Assign responsibility for contingency plans across departments
  - Prepare for various disaster types (e.g., natural disasters, cyberattacks)
  - Ensure resources and procedures for critical activities during disruptions
- **Facility security plan:** Protecting facilities and equipment from unauthorized access, tampering, and theft. Organizations should:
  - Develop policies based on unique organizational needs and risk analysis
  - Incorporate security measures like surveillance cameras, alarm systems, ID badges, and security guards
  - Train workforce members, conduct annual reviews, designate responsible personnel, and test the plan's effectiveness
- **Access control and validation procedures:** Controlling and validating physical access based on individual roles or functions. Organizations should:
  - Define access policies for different roles (staff, contractors, visitors)
  - Document access points and create an IT asset inventory
  - Implement measures like sign-in/sign-out procedures, electronic key cards, and monitored access areas
- **Maintenance records:** Documenting repairs and modifications to physical security components. Organizations should:
  - Record details such as date, description, location, reasons, responsible individuals, and follow-up actions
  - Adapt documentation methods based on organizational size (e.g., logbooks for small entities, databases for larger ones)

OCR enforcement and consequences

The newsletter notes that failure to secure facility access controls can lead to breaches and OCR enforcement. It spotlights Fresenius Medical Care Holdings, Inc. (FMC), which entered into a $3.5 million settlement for multiple potential HIPAA violations related to stolen equipment and inadequate facility access controls. FMC's potential violations included incomplete risk analysis, lack of encryption for ePHI, inadequate policies for hardware and electronic media, poor incident response procedures, and failure to secure facilities and equipment.

The implications are clear: Noncompliance with the Security Rule can lead to significant financial penalties, mandatory corrective actions, and reputational damage.

Facility access controls should integrate seamlessly with overall cybersecurity and HIPAA compliance programs.

Leaders should regularly review and update security plans to address evolving threats and environmental risks, such as natural disasters. Finally, organizations should remember that effective facility access controls not only secure sensitive areas but also support recovery efforts during emergencies through robust contingency planning.

Q&A on facility access controls

Jonathan Steele, a cybersecurity consultant at Steele Fortress and a practicing attorney for Beerman Law, caught up with **BOH** on this topic.

Q: How do you define facility access controls under the HIPAA Security Rule, and why are they critical in today's cybersecurity landscape?

A: Facility access controls, as defined under the HIPAA Security Rule, refer to the policies and procedures that limit and grant physical access to electronic information systems and the facilities in which they are housed. These controls are important because they safeguard against unauthorized physical access to sensitive ePHI. As cyberthreats continue to evolve, physical security remains a critical layer of defense to protect ePHI from breaches that could result from unauthorized physical access to devices, servers, and networks.

Q: Can you provide examples of how healthcare organizations can effectively implement contingency operations procedures during emergencies, particularly to maintain secure physical access to ePHI?

A: Effective implementation of contingency operations involves several key steps. For instance, healthcare organizations can designate secure access points and ensure they are protected even during emergencies. This includes having backup power sources like generators to maintain electronic locks and surveillance systems. Organizations should also establish clear roles and responsibilities for staff during emergencies, ensuring that only authorized personnel can access critical areas. Additionally, creating redundant access methods, such as alternative entry points, and maintaining a roster of staff who can be called upon to support facility access during an emergency are crucial practices as well.

Q: What are the key considerations when developing a facility security plan to protect ePHI, especially in facilities with shared spaces or multiple departments?

A: Key considerations include conducting a thorough risk assessment to identify potential vulnerabilities in shared spaces, implementing access control systems that restrict entry based on roles, and ensuring that all departments are aligned with the facility security plan. The plan should also include detailed protocols for visitor management, regular audits of access logs, and collaboration with building management to ensure that shared infrastructure complies with the facility's security requirements. Regular training for staff on the importance of physical security and how to report suspicious activity is also essential.

Q: How should healthcare entities adjust their facility access controls to account for increased risks due to natural disasters or other emergencies? Can you share any best practices for ensuring continuity of access to critical systems during such events?

A: Healthcare entities should adapt their facility access controls by incorporating disaster-specific protocols, such as securing backup physical access methods (e.g., manual key overrides) and ensuring that emergency power sources can sustain security systems. Best practices include conducting regular drills that simulate disaster scenarios to test the effectiveness of the controls, maintaining a clear communication plan for informing staff about access changes, and partnering with local law enforcement or emergency services to secure the facility during widespread emergencies.

Q: The HHS newsletter highlights the significant risk posed by stolen equipment containing ePHI. What strategies should healthcare entities adopt to minimize this risk, and how should they respond if such a breach occurs?

A: To minimize the risk of stolen equipment, healthcare entities should implement strong physical security measures such as lockable storage for devices, surveillance systems, and strict check-in/check-out procedures for equipment. Encrypting data on devices, even those used within secured facilities, is also crucial. In the event of a breach, immediate steps should include notifying affected individuals, conducting a thorough investigation to determine the scope of the breach, and reporting the incident to the appropriate regulatory bodies. Implementing corrective actions, such as enhancing physical security measures and revising access control policies, is also necessary.

Q: What are the best practices for implementing role-based access control and validation procedures in healthcare facilities to ensure only authorized personnel can access sensitive areas?

A: Best practices for implementing role-based access control include conducting detailed role analyses to determine the minimum necessary access each role requires, using multifactor authentication to validate access attempts, and regularly reviewing and updating access controls based on changes in roles or responsibilities. It is also essential to log all access attempts and audit these logs periodically to detect and respond to unauthorized access attempts.

Q: How important is it for healthcare organizations to document and retain maintenance records related to facility access controls, and what common mistakes should they avoid in this process?

A: Documenting and retaining maintenance records is crucial for ensuring accountability and demonstrating compliance with HIPAA regulations. Common mistakes to avoid include failing to document all maintenance activities, neglecting to update records promptly, and not securely storing these records. Healthcare organizations should establish clear procedures for recording the details of maintenance activities—including dates, times, and personnel involved and ensure these records are easily accessible during audits or in the event of an incident.

Q: What lessons can be learned from recent OCR enforcement actions related to facility access controls, and how can healthcare entities proactively address these vulnerabilities to avoid penalties?

A: Recent OCR enforcement actions highlight the importance of conducting thorough risk assessments and implementing comprehensive facility access controls that address identified vulnerabilities. Healthcare entities can proactively address these vulnerabilities by regularly reviewing and updating their security policies, ensuring all staff are trained on the importance of physical security, and conducting regular audits to identify and address any gaps in their security posture. Additionally, maintaining detailed records of all security measures and incidents can help demonstrate compliance and reduce the risk of penalties.

Q: How should facility access controls be integrated with a healthcare entity's broader cybersecurity and HIPAA compliance programs to ensure a comprehensive approach to protecting PHI?

A: Facility access controls should be integrated with cybersecurity and HIPAA compliance programs by ensuring that physical security measures are aligned with overall data protection strategies. This includes coordinating efforts between physical security teams and IT security teams, conducting joint risk assessments, and implementing controls that address both physical and cyberthreats. For example, access to data centers should be restricted to authorized personnel, and these restrictions should be reflected in both physical access control systems and network access controls.

Q: With the evolving nature of cyberthreats and the increasing occurrence of natural disasters, how should healthcare organizations adapt their facility access controls to stay ahead of these challenges?

A: Healthcare organizations should adapt their facility access controls by staying informed about emerging threats and regularly updating their security policies and procedures accordingly. This includes investing in advanced security technologies such as biometric access controls, conducting regular threat assessments, and implementing flexible access control measures that can be quickly adjusted in response to new threats. Additionally, organizations should establish strong partnerships with emergency services and cybersecurity experts to ensure they are prepared to respond to any type of disaster or security incident.